UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

VERIFIED IDENTITY PASS, Inc., d/b/a/ CLEAR REGISTERED TRAVELER, Plaintiff,	:	07 Civ. 6538 (JGK)
-against-	:	
FRED FISCHER, SAFLINK CORPORATION, and FLO CORPORATION, Defendants.	:	

DEFENDANTS' MEMORANDUM OF LAW IN OPPOSITION TO PLAINTIFF'S REQUEST FOR A TEMPORARY RESTRAINING ORDER

DLA PIPER US LLP
1251 Avenue of the Americas
New York, New York 10020-1104
(212) 335-4500

Attorneys for Defendants Fred Fischer, Saflink Corporation, and FLO Corporation

Of Counsel:
Stanley McDermott III (SM 0530)
Michael R. Hepworth (MH 2398)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

OTHER AUTHORITIES

Defendants Fred Fischer, Saflink Corporation ("Saflink") and FLO Corporation ("FLO"), partially owned by Saflink, oppose the request for a temporary restraining order by plaintiff Verified Identity Pass, Inc. ("Verified"). Also submitted are declarations from Fred Fischer, FLO's Senior Vice President, Luke Thomas, FLO's Executive Vice President, and Kevin Mitchell, the Chairman of Business Travel Coalition, Inc.

PRELIMINARY STATEMENT

By this action Verified seeks to prevent Fischer, Saflink, and FLO from competing in the rapidly developing market for "Registered Traveler" cards—the Government-approved biometrically-encrypted "smart" cards that expedite entry through airport security. Verified's meritless application for a temporary restraining order ("TRO") aside, the pleaded facts do not begin to state a valid claim under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.*, and this Court perforce lacks subject matter jurisdiction. Even if Verified were arguably to state a CFAA claim, which it cannot do, this Court would still be compelled to decline to exercise supplemental jurisdiction over the various state-law claims—breach-of-contract, misappropriation, tortious interference, conversion, and deceptive practices—that by a wide margin "substantially predominate" over any notional and unsustainable CFAA claim. *See* 28 U.S.C. § 1367(c)(2).

The incurable jurisdictional deficiencies aside, Verified's application does not justify any TRO. Verified alleges that Fred Fischer—formerly head of RT-card sales at Verified, now head of RT-card sales at FLO—has misused confidential information from Verified's so-called "Salesforce Database." But the facts show no such confidential information and no misuse.

The basis for Verified's claim is a 6-page list (the "List") of names from the Salesforce Database that Fischer printed on December 5, 2006, his last day of work at Verified. The List (Exhibit A to the Declaration of Fred Fischer) contains contact information for Government officials, Senators, Congressmen, airport executives, and the managers of travel-related services

for the major corporations likely to be interested in acquiring or branding RD cards. This Court has only to cast its eyes down that List to see that these kinds of names are not "trade secrets." Any experienced travel-services salesman could compile similar lists with minimal effort.

Fischer himself provided virtually all the names of the corporate travel managers on the list *to* Verified, and he cannot be barred from using what he knew before he ever worked for Verified. Neither can he be liable for violating the CFAA by seeking to access Verified's database, which is actually stored on the servers of "Saleforce.com," a web-based information-management provider. On Verified's own evidence, Fischer lacked an active password, and therefore on the dates alleged *could not and did not gain access to Verified's database.*

What is more, the overbroad and impermissibly vague wording of the proposed TRO—restraining the defendants from "soliciting for business any and all individuals and corporations affiliated with individuals whose contact information was contained on plaintiff's Salesforce Database for a period of six months" (*see* Order to Show Cause)—would, if granted, allow Verified to virtually monopolize the RT market and suppress legitimate competition. Verified's overblown request for a TRO—which does even identify the individuals and companies said to be on the undisclosed Database—must be denied because there is no probability it might succeed on the merits and it is not threatened with irreparable harm of any kind.

FACTS

A. The Parties.

A full narrative of the material facts is provided in Mr. Fischer's declaration submitted on this motion. In sum, Mr. Fischer has 30 years experience in the travel industry. Among other things, for 8 years (1996 to 2003) he held senior positions developing American Express's premium corporate-card and corporate travel-services business. He joined Verified on December 5, 2005 to head its efforts to promote its Registered Travel ("RT") business to the major corporations

likely to buy or promote the "RT cards" that are encrypted with biometric data and expedite a cardholder's access through airport security.

Verified is a small company organized in 2004 to take advantage of the RT program being developed by the Department of Homeland Security's Transportation Security Administration ("TSA") in the aftermath of 9/11. Fischer spent one year at Verified until he was terminated as of December 5, 2006. During those 12 months he was Verified's only marketing arm to the major corporations to whom Verified sought to promote its RT Cards (assisted for a brief period by a junior sales assistant). (Fischer Decl. ¶¶ 2, 17.) Fischer brought to Verified his wealth of industry contacts, which is why Verified hired him. Virtually all the contacts Fischer focused on while at Verified were known to him before he joined Verified. (Fischer Decl. ¶¶ 6, 26, 33.)

FLO, partially owned by Saflink, is a leading encryption-technology provider. It is Verified's chief competitor in the burgeoning RT business. (Fischer Decl. ¶¶ 22, 23.) When he left Verified Fischer had not had any contact with FLO. (*Id.* ¶ 43.) Since March 2007 he has headed up FLO's efforts to market its RT cards and RT services to major corporations.

B. The Developing Registered Traveler Business.

As Verified's complaint notes (Cmplt. ¶ 11), RT providers like Verified and FLO operate RT programs in conjunction with the TSA. The RT provider issues an RT card encrypted with the cardholder's personal biometric data (fingerprint and iris scan), the TSA approves the cardholder, and the cardholder presents the card at designated RT lanes to gain expedited access through airport security. The RT business has two main parts. (Fischer Decl. ¶ 20.) On one side of the business the RT provider contracts with airports and airlines to open the special-purpose "RT lanes" at airline terminals. On the other side of the business the RT provider markets its cards to the major corporations expected either to buy RT cards in large volumes or perhaps partner with

the provider to develop RT-branded services. Fischer worked only on the latter side of the business at Verified and does so today at FLO. (*Id.* ¶ 20.)

The targeted customers for RT card sales and services are the major corporations and large travel-services companies (*e.g.*, hotel chains, rental-car companies, and credit-card issuers) known to everyone in travel industry. (Fischer Decl. ¶ 21.) The contacts at those companies are the travel-services managers who are readily identifiable by anyone experienced in the travel industry.

The suggestion throughout Verified's papers that its list of such names is closely-guarded, confidential information borders on the frivolous. (*See* Cmplt. ¶¶ 18-21.) Anyone with experience in the travel industry could readily identify (and list) the travel managers of the large corporations likely to be interested in acquiring or promoting RT cards and RT services. (Fischer Decl. ¶ 9.)

C. Verified's "Salesforce Database" and the List Printed by Fischer.

The heart of Verified's misperceived action is the allegation that Fischer, on December 5, 2006, wrongly "downloaded" to an Excel spreadsheet Verified's allegedly proprietary list of major corporate contacts. (Cmplt. ¶ 26.) What Fischer did, however, is simply print on December 5, 2006 a portion of Verified's customer-contact list. That printout (the "List") is Fischer Decl. Ex. A. Mr. Fischer has explained what the List is—a roster of readily identifiable persons scattered across Government, Congress, national airports, and the travel industry. (Fischer Decl. ¶¶ 4, 8, 31, 32.) A mere glance at the List refutes Verified's assertions that such information is "trade secret."

The List has two parts. The first part — the first 64 names on pages 1 and 2 — consist of the names and contact details of Government agency officials, Senators, Congressmen, airport officials and public relation consultants. (Fischer Decl. ¶ 31.) There is nothing confidential or proprietary about such information. (*Id.*)

The second part—the next 108 names running from the bottom of page 2 to the top of page 6 — consists largely of travel managers of large corporations likely to be interested in buying or

promoting RT cards and services. (Fischer Decl. ¶ 32.) Not only is such contact information readily obtainable and not proprietary, but Mr. Fischer himself provided all but *four* of those names to Verified. (*Id.* ¶¶ 6, 8, 9, 11, 33.)

As Fischer also explains, Verified started the "Salesforce Database" ("Database") sometime in 2006 when a young sales assistant, Bates Gregory, suggested using the web-based "Salesforce.com" information-management technology. (Fischer Decl. ¶ 7.) The Database is stored on the Salesforce.com servers and is accessible only by Verified-authorized passwords. While Fischer provided names for the Database, he did not use it for day-to-day business. (*Id.* ¶ 7.)

Although the first pillar of Verified's "Computer Fraud and Abuse Act" claim is Fischer's accessing of the Salesforce.com site on December 5, 2006 to print the List (Fischer Decl. Ex. A), there is nothing the slightest bit wrong about Fischer's printing of the List on that date. When Verified (on December 4, 2006) terminated Mr. Fischer as of December 5, 2006, Verified asked Fischer to continue to lend assistance during a 30-day severance or transition period. (Fischer Decl. ¶¶ 5, 17, 28.) As later emails show, Verified expected Fischer to continue to share contact information, Fischer did so, and Verified even kept open the possibility that Fischer might work on future projects. (Fischer Decl. ¶¶ 17, 38-40, Exs. D, E, F.) The List would help Fischer do what Verified wanted him to do in the transition period. Fischer was authorized to use his still-active Verified password to print the List on December 5, 2006, and no one told him not to do so. (*Id.* ¶ 36.) Although Verified suggests that Ms. Beer inactivated Mr. Fischer's Salesforce.com password shortly after he was terminated, her evidence (Beer Aff. Ex. B) indicates she did so only 30 days after December 5, 2006, when she modified Fischer's password access on January 4, 2007.

D. The Alleged Clicks on Salesforce.com.

Equally insignificant is the second pillar of Verified's CFAA claim, the assertion that Fischer on four later dates (January 31, 2007, April 6, 2007, June 12, 2007, and June 19, 2007)

sought to access Database on the Salesforce.com site, even though he concededly could not and did not access the Database on those dates because he lacked an active password. (*See* Cmplt. ¶ 40; Beer Aff. ¶ 12, and Beer Aff. Ex. A.) Verified claims to have discovered Fischer's admittedly *unsuccessful* contact with the Salesforce.com servers after "investigating" a July 10, 2007 email message sent by Kevin Mitchell of Business Travel Coalition, Inc. ("BTC"), an industry consultant known to Verified, to BTC's circulation database. (Brill Aff. ¶¶ 34-35.) (That email is further explained below.) Fischer, however, denies having sought to access Verified's Database on those dates (Fischer Decl. ¶¶ 12, 13, 44; Thomas Decl. ¶ 6), and Verified in all events sustained no harm because Fischer, lacking an active password, did not access the Database on those dates.

It is possible that Fischer simply clicked inadvertently on the "Salesforce.com" icon on the toolbar of his laptop, which would account for the incidents in question. As he explains (Fischer Decl. ¶¶ 12, 13, 44), since he had initially (in 2006) entered his username and password to access Verified's Salesforce.com account, any inadvertent click on the Salesforce.com icon on his computer (in 2007) would probably have automatically caused the Salesforce.com server to try to log him onto Verified's account using the same username and password saved in his computer's memory. But because his user code was inactive on the four dates in question (Beer Aff. Ex. A), by clicking on the "Salesforce.com" icon Fischer could not (and did not) gain entry to the Database. In all events Verified does not plead facts showing that Fischer ever attempted to "hack" into its computer systems or that its computer operations have been damaged, impaired or interrupted.

E. The Mass Emailings by Nonparty Mitchell.

Verified also seriously misstates the facts by suggesting that Fischer, FLO and Saflink sent a series of three email messages on July 5, 2007, July 10, 2007, and July 14, 2007 for some unexplained anti-competitive purpose. (*See* Cmplt. ¶¶ 41-43; Beer Aff. ¶¶ 13-16; Brill Aff. ¶¶ 28, 32.) These emails (Beer Aff. Exs. C, D, E, and F) were sent by Kevin Mitchell, the head of BTC and

the manager of the leading travel-industry web-site, www.businesstravelcoalition.com, to a BTC circulation base of more than 10,000 subscribers. (Fischer Decl. ¶ 48; Mitchell ¶¶ 2, 12-15.)

Kevin Mitchell is a leading travel-industry expert and independent consultant who for one year provided consulting services to Verified (April 2005 to April 2006) and is now providing similar services to FLO. (Fischer Decl. ¶¶ 27, 47; Mitchell Decl. ¶¶ 5, 6, 7, 10.) Fischer first began working with Mitchell in December 2005 when Fischer started with Verified and Fischer continues to consult with Mitchell today on FLO's behalf. (*Id.*)

Verified contends that Fischer has seeded BTC's extensive circulation database with email addresses of individuals on Verified's Database, but Fischer denies doing so (Fischer Decl. ¶ 47), and Mitchell supports Fischer's denial. (Mitchell Decl. ¶¶ 2, 16.) Given the nature and large size of BTC's circulation base, compared to the 174 names on the List, there is no basis for claiming that these emailings targeted Verified's contacts.

As Fischer and Mitchell explain, the three emails do not concern Verified. The first (July 5th) (Beer Aff. Exs. C and H) previewed a magazine article written by Mitchell for an industry periodical. (Fischer Decl. ¶ 49; Mitchell Decl. ¶ 12, 13.) Mitchell sent that message to 10,578 email addressees in BTC's database. (Mitchell Decl. ¶ 12.) The second (July 10th) (Beer Aff. Ex. D) informed readers of a BT-card discount offered by FLO at the time. (Fischer Decl. ¶ 50; Mitchell Decl. ¶ 14.) Mitchell sent that message to 10,237 email addresses in BTC's database. (Mitchell Decl. ¶ 14.) The third (July 16th) (Beer Aff. Ex. E) invited readers to participate in a survey conducted by BTC on FLO's behalf. (Fischer Decl. ¶ 51; Mitchell Decl. ¶ 15.) Mitchell sent that message to the same database of 10,578 email addresses to which sent the July magazine article. (Mitchell Decl. ¶ 15.) None of these email messages, sent in the ordinary course of BTC's business, could possibly be said to harm Verified.

F. The Little Rock Airport Hearing.

Verified claims that at a public hearing before the Little Rock Airport Commission on April 11, 2007, Fischer violated his employment agreement by disclosing confidential and proprietary information he learned while employed at Verified. (Cmplt. ¶ 31; Brill Aff. ¶¶ 17-18.) Verified's accusations are meritless, as Verified's own submissions on this motion show.

The Complaint alleges that Fischer disclosed Verified's secret "revenue sharing formula and method" when Fischer made a statement that began "'As far as I know from working for our competitor . . . .'" (Cmplt. ¶ 31, with ellipsis as in the Cmplt.) But what Fischer said is revealed in the transcript that is attached to Verified's court filing and shows nothing improper. What Fischer said was "As far as I know from working for our competitor you will get revenue for just the airport." (Brill Aff. at Ex. D, at p. 30.) This does not reveal any secret "revenue sharing formula and method," and in any event what Verified proposed to the Little Rock Airport Commission is, of course, known to the Commission. According to the transcript one Commission member immediately responded to Fischer's statement by saying "That's right." (*Id.*) It was not a secret to them. It is not a secret to anyone after Verified included it in its public filing with this Court.

The Complaint also alleges that Fischer revealed "how corporate travel managers regard the idea of reimbursing employees for a Registered Traveler card" because he had seen over 250 corporate travel managers across the country. (Cmplt. ¶ 31.) But an employee cannot be barred from using the general experience he learns in the course of his employment. This is not a protectable secret, and Verified has now made the information public in its court papers.

The Complaint also alleges that Fischer revealed confidential information to the Little Rock Commission when he told the commission it would "'hear from our competitors' that they will only set up remote kiosks to sign up customers for the Registered Traveler Program, if a company will have a minimum of 250 people to enroll." (Cmplt. ¶ 31.) But Fischer cannot be

barred from asking the Commission to consider whatever it was that Verified proposed. And as with all these accusations, Verified has now made the information public.

G. Verified's Tactical Litigation to Suppress Competition.

Verified's aim to suppress competition is plain. As Fischer and Mitchell note, competition between Verified and FLO, the leading RT providers, is intensifying. (Fischer Decl. ¶ 22, 23; Mitchell Decl. ¶ 4.) The RT business, slow to get started, is gaining speed rapidly on the back of the TSA program rules released earlier this year. (Fischer Decl. ¶ 18, 19, 24; Mitchell Decl. ¶ 4.) More and more airports will soon contract for RT lanes with RT providers. More and more major corporations will buy RT cards. And more and more hotels chains, rental-car companies and credit-card issuers to promote their services will team up with RT-card issuers. It is hardly a coincidence that Verified filed its meritless action shortly before the oral presentations that Verified and FLO (and only they) were scheduled to make yesterday before the Washington, D.C. airport authority, one of the airports most important to RT providers. (Fischer Decl. ¶ 23.)

ARGUMENT

I. This Court Lacks Subject Matter Jurisdiction.

The CFAA is primarily a criminal statute designed to prevent unauthorized access that impairs the physical integrity of protected computers. 18 U.S.C. §§ 1030(a), (b), and (c). It was amended in 1994 to create a limited civil right of action for violations of certain prescribed CFAA provisions, 18 U.S.C. § 1030(g). (For the Court's convenience we have appended the text of the CFAA as Exhibit A.) There are significant hurdles, however, to pleading a civil cause of action. There must be "unauthorized access" that causes actual "damage" and actual "loss."

Verified's CFAA claim is grounded in (a) Fischer's allegedly unauthorized "downloading" of the "Salesforce Database" on December 5, 2006 and (b) the four alleged incidents (January 31, 2007, April 6, 2007, June 12, 2007, and June 19, 2007) when Mr. Fischer allegedly clicked on the

Salesforce.com web site but did *not* gain access to the Database because Verified had earlier inactivated his password. Neither of these events, however, concerns the threefold showing of "unauthorized access," "damage" and "loss" required to state a civil claim under § 1030(g).

Indeed, it is apparent that Verified is simply trying to manufacture Federal jurisdiction to support the five state-law claims that are the actual, if meritless, bases for the requested injunctive relief. But if printing a lawfully downloaded contact list and clicking on a blocked web site were actionable under the CFAA, the Federal courts would be flooded with actions having nothing to do with the sort of computer "hacking" that the CFAA actually addresses.

Verified's failure to plead a CFAA claim is evident when the statute is parsed. The starting point is § 1030(g): "[a] civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B)" [*i.e.*, §§ 1030(a)(5)(B)(i)-(v)].

Section 1030(a)(5)(B)(i) extends to "conduct described in clause (i), (ii), or (iii) of subparagraph (A)" that "cause (or, in the case of an interrupted offense, would, if completed, have caused)—

> (i) *loss* to one or more persons during any 1-year period * * * aggregating at least $5,000 in value.

"*Loss*" is a defined term, § 1030(e)(11), and includes:

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, and other consequential damages incurred because of interruption of service.

Before one can assess whether there has been "loss" under §§ 1030(a)(5)(B)(i) and 1030-(e)(11), however, one must look first to the incorporated provisions of § 1030(a)(5)(A)(i)-(iii). A *loss* will be at issue only if it is *caused* in one of the ways listed in these sections of the statute.

But none of these three sections is applicable. Each section prohibits conduct by which one intentionally accesses a protected computer *without authorization* and thereby causes *damage*.

- Section (a)(5)(A)(i) applies when someone "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."

- Section (a)(5)(A)(ii) applies when someone "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage."

- Section (a)(5)(A)(iii) applies when someone "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage."

"*Damage*" is also a defined term, § 1030(e)(8), and means:

"any impairment to the integrity or availability data, a program, a system, or information."

In the light of these sections of the statute, Verified must show three things to state a civil cause of action under § 1030(g):

First, Verified must show that Fischer violated § 1030(a)(5)(A) by first *intentionally accessing a protected computer without authorization*. Second, Verified must show that such access *damaged* the integrity of data systems, programs or information on that computer. Third, Verified must show that, as a result of such damage, it sustained a *loss* under § 1030(a)(5)(B)(i) and § 1030(e)(11).

Verified cannot satisfy any of these three prongs of the CFAA standard—unauthorized access, damage, and loss—whether one considers (a) Fischer's actions in printing the List on December 5, 2006 or (b) Fischer's later clicking on the Salesforce.com icon allegedly to access the "Salesforce Database" stored on the Salesforce.com servers.

A. *Printing the List*. Printing the List on December 5, 2006 did not conceivably violate the CFAA because Fischer had *authorized* access to the "Salesforce Database" on that date,

printing the List did not *damage* any computer data, program, system or information, and Verified did not sustain any *loss* as a result of any unauthorized access and any resulting damage.

B. *The Clicks on Salesforce.com.* Clicking unsuccessfully on Salesforce.com in a failed attempt to access Verified's "Salesforce Database" also did not and could not violate the CFAA because Fischer did not thereby *access* a protected computer (to the contrary, access was blocked), cause *damage*, and cause *loss*. As noted, it is likely that Fischer simply inadvertently clicked on the Salesforce.com icon on the tool bar of his laptop computer on the scattered dates in question. (*See* Fischer Decl. ¶¶ 12, 13, 44.) Regardless, an *unsuccessful* effort to access the web-based Salesforce.com site in order to access the Database on that site (even if deliberate) cannot violate the CFAA when access is password-blocked and there is perforce no resulting damage and loss.

Indeed, were that not the case then any click on a password-protected site would instantly confer Federal criminal and civil jurisdiction even though the password block worked as intended, access to the site was thereby denied, and the site holder was not adversely affected in any way.

C. *Verified's Insufficient Pleading.* As explained above, Verified can state a claim only if it alleges the three requisite elements of a CFAA claim in accordance with § 1030(a)(5)(B). Verified has not done this. Instead, it alleges (without explaining) that Fischer violated 18 U.S.C. §§ 1030(a)(2)(C), (a)(4), and (a)(5), and that Saflink and FLO, "through Fischer's acts," violated § 1030(a)(5). (Cmplt. ¶¶ 53-54.)

This is plainly insufficient, as is evident when these sections of the statute are reviewed:

1. *§§ 1030(a)(2)(C).* Subsection § 1030(a)(2)(C) concerns someone who "intentionally accesses a computer without authorization or exceeds authorized access" and obtains "information from any protected computer if the conduct involved an interstate or foreign communication." Pleading §§ 1030(a)(2)(C) is irrelevant, however, because it is not incorporated

into § 1030(a)(5)(B) for purposes of a civil action under § 1030(g). To plead a valid CFAA cause of action, the plaintiff must specifically plead a violation of § 1030(a)(5)(B) (and necessarily a violation of the incorporated § 1030(a)(5)(A)(i)-(ii)). *See e.g., B.U.S.A. Corp. v. Ecogloves, Inc.*, No. 05 Civ. 9988 (SCR), 2006 WL 3302841, at *2 n.5 (S.D.N.Y. Jan. 31, 2006) ("Because section 1030(g) limits civil actions to conduct that involves one of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of section 1030(a)(5)(B), this Court cannot grant a preliminary injunction based on Plaintiffs' claims under sections 1030(a)(2)(C) and (a)(4).").[1]

2. *§§ 1030(a)(4).* Section 1030(a)(4) concerns someone who with intent to defraud accesses a protected computer without authorization and thereby furthers the fraud. Verified does not plead fraud or an intent to defraud. Pleading § 1030(a)(4) is equally irrelevant because it also is not incorporated into § 1030(a)(5)(B) for purposes of a civil action under § 1030(g). *McLean v. Mortgage One & Fin. Corp.*, No. Civ. 04-1158, 2004 WL 898440, at *2 (D. Minn. Apr. 9, 2004) ("[The CFAA] limits civil enforcement to actions claiming a violation of § 1030(a)(5)(B), not § 1030(a)(4). Thus, [defendant] cannot maintain a civil action on its claims for a violation of § 1030(a)(4), and is therefore not likely to succeed on its [CFAA] claims.")[2]

---

[1] Fischer was plainly authorized to print the List on December 5, 2006. *See e.g., Lockheed Martin Corp. v. Speed*, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006) ("Because [plaintiff] permitted the Employees to access the company computer, they were not without authorization. Further, because [plaintiff] permitted the Employees to access the precise information at issue, the Employees did not exceed authorized access."). Any allegation that Fischer might later have *used* the information improperly does not implicate the CFAA. *See Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 498-499 (D. Md. 2005) (potentially improper use of information does not mean that defendant was not authorized to access the information or exceeded her authorization in violation of the CFAA).

[2] Under § 1030(a)(4), as under § 1030(a)(2)(C), unauthorized access is not tantamount to unauthorized use. *See Brett Senior & Associates v. Fitzgerald*, No. Civ. A. 06-1412, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007) (noting that § 1030(a)(4) says "exceeds authorized access," not "exceeds authorized use").

3. *§ 1030(a)(5)*. Pleading *§ 1030(a)(5)* is likewise purposeless when the statutory prerequisites cannot be met, *i.e.*, there has been no *unauthorized access*, no *damage* to computer data, programs, systems, or information, and such damage has not in turn caused *loss*.

4. *Verified has not sustained Loss*. Unable to plead the requisite unauthorized access, unable to plead the requisite damage, Verified evidently considers it sufficient only to plead "loss." But "loss" alone is insufficient and Verified has not sustained any loss.

Verified claims to have sustained a statutory "loss" because it has spent money investigating Mr. Fischer (Cmplt. ¶ 55). Verified hired Kroll, however, only after learning that Mr. Fischer had *not* gained access to and had *not* damaged Verified's Database. (*See* Beer Aff. ¶ 12 and Beer Aff. Ex. A.) The assertion that Kroll is nonetheless determining "the extent of Mr. Fischer's intrusion into our system, and to assess and remediate any damage to the system and to implement remedial safeguards to the system" (Beer Aff. ¶ 12) is poppycock. There is *no* evidence of unauthorized access or "intrusion," *no* evidence of any statutory "damage," and *no* evidence of any need for remedial safeguards against nonexistent damage. As a result, there can be no "loss."

While "loss" under § 1030(e)(11) may include a variety of costs, such costs must still be the result of actual damage or an "interruption of service." In other words, to meet the definition of "loss" under § 1030(e)(11), the computer must have been accessed without authorization and there must have been an "offense" that physically impaired data, a program, a system, or information. Nothing like that happened here. As noted in *Civic Center Motors, Ltd. v. Mason St. Import Cars, Ltd.*, "'losses' under the CFAA are compensable only when they result from damage to, or the inoperability of, the accessed computer system." 387 F. Supp. 2d 378, 381 (S.D.N.Y. 2005); *accord Nexans Wires S.A. v. Sark-USA, Inc.*, 166 Fed. Appx. 559, 562-563 (2d Cir. 2006) (upholding grant of summary judgment dismissing CFAA claims because there was no "interruption of service"); *see also Chris S. Winner, Inc. v. Polistina*, No. Civ. A. 06-4865, 2007 WL 1652292,

at *4 (D.N.J. June 4, 2007) (finding plaintiffs' statement that they hired a computer expert to conduct an assessment and investigation insufficient to show that plaintiffs could prove loss under the CFAA). Having failed to show *unauthorized access*, having failed to show *damage*, Verified also cannot show the requisite *loss*.[3]

Count I must therefore be dismissed and with it the complaint as a whole.

II. This Court Should Not Exercise Supplemental Jurisdiction.

Even if this Court were arguably to have CFAA jurisdiction, which it does not have, the Court would still be compelled to decline to exercise supplemental jurisdiction over Verified's state-law claims [Counts II (Breach of Contract Against Fischer), Count III (Misappropriation of Trade Secrets Against All Defendants), Count IV (Tortious Interference with an Existing Contract Against Saflink and FLO), Count V (Conversion Against Fischer) and Count VI (Deceptive Practices Against All Defendants)].

In accordance with 28 U.S.C. § 1367(c)(2), the Court may decline to exercise supplemental jurisdiction over any state-law claim that "substantially predominates over the claim or claims over which the district court has original jurisdiction." Here the gravamen of Verified's complaint and requested injunctive relief is far and away the state-law claims, not the feeble CFAA claim that is simply a pretext for Federal jurisdiction.

---

[3] Despite the statute's plain wording, some courts have given § 1030(g) an expansive reading and allowed civil claims for alleged violations of sections other than those listed in § 1030(a)(5)-(B), but these cases still require the claimant to allege one of the five enumerated factors in § 1030(a)(5)(B). *See I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 526 (S.D.N.Y. 2004); *P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504, 511-512 (3d Cir. 2005). Verified cannot rely on *Kaufman v. Nest Seekers, LLC*, No. 05 CV 6782(GBD), 2006 WL 2807177 at *8 (S.D.N.Y. Sept. 26, 2006) to suggest that a party can plead loss without actual damage to the computer system as *Kaufman* concerns a massive criminal attack with unauthorized access by over 4,000 logins, causing the plaintiff to expend over $125,000 in investigation costs. *Id.* at *2-3.

"In determining whether state law claims predominate, courts consider the type of proof necessary, the comprehensiveness of remedies, and the scope of the issues raised." *Dunlop v. City of New York*, No. 06-CV-433, 2006 WL 2853972, *5 (S.D.N.Y. Oct. 4, 2006) (citing *Surprise v. GTE Serv. Corp.*, 47 F. Supp. 2d 240, 243 (D. Conn. 1999)). Thus, "courts in this district have found that state law claims predominate when the federal law claims are merely peripheral or cover a much narrower issue than the state law claims, or where the factual or legal analysis of the claims are unrelated." *Id.* at *5. Here, the CFAA claim is far narrower than the breach-of-contract, misappropriation, tortious-interference, conversion, and deceptive-practices claims that are the actual, if meritless, grounds for the proposed injunctive relief. And the misuse of information acquired during the course of employment is governed by state law, not the CFAA. *Int'l Ass'n of Machinists*, 390 F. Supp. 2d at 498-499.

Likewise the "factual or legal analysis" of the CFAA and the five state-law claims is substantially "unrelated," the more so when Verified is seeking to prevent the Defendants from using information that Fischer allegedly obtained at Verified. And there is no threatened CFAA violation in prospect. Verified's evidence shows that Fischer, lacking an active password, cannot access the Database on the Salesforce.com servers, and Fischer has never hacked into or damaged Verified's computer network. It follows that the grounds for declining to exercise supplemental jurisdiction over the state-law claims under 28 U.S.C § 1367(c)(2) eclipse by far any Federal interest under the CFAA.

III. There Is No Basis For Issuing A TRO.

To prevail on a motion for preliminary injunctive relief or TRO, the party seeking relief must establish "(1) irreparable harm in the absence of the injunction and (2) either (a) a likelihood of success on the merits or (b) sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly in the movant's favor."

MyWebGrocer, LLC v. Hometown Info, Inc., 375 F.3d 190, 192 (2d Cir. 2004) (quoting *Merkos L'inyonei Chinuch, Inc. v. Otsar Sifrei Lubavitch, Inc.*, 312 F.3d 94, 96 (2d Cir. 2002)).

As explained below, Verified cannot meet any part of this test.

A. There is no likelihood that Plaintiff will succeed on the merits of its claim under the Computer Fraud and Abuse Act.

As explained above in Point I, neither Fischer's authorized December 5, 2005 printout nor the later incidents whereby access to the Salesforce.com website was blocked support a CFAA cause of action. Verified has not pleaded a sustainable civil right of action under the interrelated provisions of 18 U.S.C. § 1030(g), § 1030(a)(5)(B)(i), and § 1030(a)(5)(A)(i)-(iii), Verified has not sustained any statutory "damage," 18 U.S.C. § 1030(e)(8), and Verified has not sustained any statutory "loss," 18 U.S.C. § 1030(e)(11). Misusing information may give rise to contractual or common-law legal liability, but it cannot sustain a CFAA claim.

B. There is no likelihood that Plaintiff will succeed on the merits of its claim for misappropriation of trade secrets.

Verified claims Defendants misappropriated Verified's trade secrets by taking its Database on December 5, 2006, and wrongfully using the information in the Database in emailings that were distributed by a nonparty, Kevin Mitchell. (Cmplt. ¶¶ 66-70.) But there is no likelihood that Verified can succeed on this claim because no trade secret was misappropriated or misused.

To prevail under New York law for misappropriation of a trade secret, "the plaintiff must demonstrate (i) that it possessed a trade secret and (ii) that the defendant used that trade secret in breach of an agreement, a confidential relationship, or duty, or as a result of discovery by improper means." *Hudson Hotels Corp. v. Choice Hotels International*, 995 F.2d 1173, 1176 (2d Cir. 1993). The following factors are relevant in determining whether a trade secret exists:

> (1) the extent to which the information is known outside of [the] business; (2) the extent to which it is known by employees and others involved in [the] business; (3) the extent of measures taken by [the business] to guard the secrecy of the information; (4) the value

> of the information to [the business] and to [its] competitors; and (5) the amount of effort or money expended by [the business] in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Ashland Management Inc. v. Janien, 82 N.Y.2d 395, 407, 604 N.Y.S.2d 912, 918 (1993) (quoting Restatement of Torts § 757, comment b)); *see also, e.g.*, *Softel, Inc. v. Dragon Medical and Scientific Communications, Inc.*, 118 F.3d 955, 968 (2d Cir. 1997) ("New York generally looks to section 757 of the first Restatement of Torts for its definition of a trade secret.")).

As explained below, Verified cannot meet any part of this standard:

First, there was no improper taking or discovery of anything. The focus of Verified's Complaint is the List that Fischer printed on December 5, 2006, but there was nothing improper about what he did. Fischer printed the List so that he would be able to do what Verified asked him to do, which was to be ready to talk with Verified about contacts after Fischer left Verified. (Fischer Decl. ¶¶ 28-29.) This is not misappropriation; it is responding in a reasonable way to a specific request by an employer. Verified later asked Fischer to provide contact information, which Fischer provided. (Fischer Decl. ¶¶ 38-42.) When Verified requested the information from Fischer, Verified also made thinly veiled threats in late January 2007 that if Fischer did not do what Verified asked, Verified would not pay Fischer the share options that he was owed under his employment agreement with Verified. (Fischer Decl. ¶ 41.) In fact, Verified has not paid Fischer what it owes him. (*Id.*)

Second, the List is not what Verified claims. The information on the List does not contain the "notes and comments as to particular negotiations and deal" or "Customer Account" information that Verified says it is concerned about. (*See* Pl. Mem. 18, 17.) This is evident on the face of the List. (Fischer Decl. Ex. A.) Moreover, Verified's own alleged expert undermines its claim when he explains that the information accessed by Fischer on December 5, 2006 included only

"First Name; Last Name; Address; City; State; Zip Code; Country; Email Address; Account Owner; Title; Phone Number 1; Phone Number 2; Lead Source and Account Name." (A. Brill Aff. ¶ 17; *see also* Fischer Decl. Ex. A.)

Third, on its face the List also shows that Verified is wildly wrong when it characterizes the information at issue as confidential, nonpublic information that is not generally available. Roughly a third of the names on the List are government officials whose names could never be claimed as confidential trade secrets. The alleged "secret" names include "Governor Jeb Bush", the "House Homeland Security" counsel, "TSA [Transportation Security Administration]", and Senators, Congressmen and Congresswomen. (Fischer Decl. Ex. A.)

Nearly all of the first 64 names on the List are of this kind. The List marks the names with their "Contact Owner Alias" in the right-hand column. The first 64 names are associated with "csimo", which is the person at Verified (Robert Cimino) who dealt with the airport side of the business. (Fischer Decl. ¶ 31.) Almost all of those first 64 names on the List are government agencies and officials who are by their very nature public and cannot be "confidential." The few company names are well-known ("Lockheed Martin," for example).

Fourth, all of the remaining 108 names, except four, are names provided by Fischer to Verified when he came to Verified. (Fischer Decl. ¶¶ 6, 33.) The "Contact Owner Alias" on the List for these 108 names is "FFisc", *i.e.*, is Fischer. 103 out of the 108 names are ones that Fischer provided to Verified because Fischer already knew them from his long experience in the travel industry. (Fischer Decl. ¶ 6.) As explained below, as a matter of law the names known to Fischer cannot be claimed by Verified as information that it can bar Fischer from using.

A list of customers will not be protected when it is the result of the employee's own prior experience. *See, e.g., Iron Mountain Information Management, Inc. v. Taddeo*, 455 F. Supp. 2d 124, 140 (E.D.N.Y. 2006) (no protection for customer list because "In short, the list of customer

contact information was developed largely through the efforts of Taddeo [the defendant employee] both before and during his employment at Iron Mountain [the plaintiff company], in a market that is not highly specialized but has many, easily identifiable, potential customers"); *BDO Seidman v. Hirshberg*, 93 N.Y.2d 382, 391, 690 N.Y.S.2d 854, 859 (1999) (protecting only customer relationships "the employee *acquired* in the course of employment", not those he had before the employment); *SG Cowen Securities Corp. v. Messih*, 2000 WL 633434, at *6 (S.D.N.Y. May 17, 2000) (*BDO Seidman* [cited immediately above] "recognized that the employers have no legitimate interests in preventing employees from competing for the patronage of clients they have acquired independently"), *aff'd*, 224 F.3d 79 (2d Cir. 2000); *Willis of New York, Inc. v. DeFelice*, 299 A.D.2d 240, 242, 750 N.Y.S.2d 39, 42 (1st Dep't 2002) (defendant "should not be enjoined from soliciting the clients he originally brought with him to plaintiffs, or related accounts").

Verified can protect names on the List only if *it* expended substantial time, money and effort in developing the List. *Leo Silfen, Inc. v. Cream*, 29 N.Y.2d 387, 393, 328 N.Y.S.2d 423, 427 (1972). Verified did nothing to acquire the names that Fischer brought with him to Verified.

Fifth, the names of the companies on the List are all readily ascertainable and are not protectable as a trade secret. "Generally, where the customers are readily ascertainable outside the employer's business as prospective users or consumers of the employer's services or products, trade secret protection will not attach and courts will not enjoin the employee from soliciting his employer's customers." *Leo Silfen, Inc. v. Cream*, 29 N.Y.2d 387, 392, 328 N.Y.S.2d 423, 427 (1972); *see also, e.g.*, *Iron Mountain Information Management, Inc. v. Taddeo*, 455 F. Supp. 2d 124, 138 (E.D.N.Y. 2006) ("customer lists are generally not considered confidential information" (quoting *H. Meer Dental Supply Co. v. Commisso*, 269 A.D.2d 662, 664, 702 N.Y.S.2d 463 (2000)); *Hancock v. Essential Resources, Inc.*, 792 F. Supp. 924, 927 (S.D.N.Y. 1992) (denying preliminary injunction because, *inter alia*, potential customer contact list was easily created).

Verified claims that although the company names may be well known, the specific contacts at those companies may be protected. But here the specific contacts were previously known to Fischer, or could easily be found simply by calling the companies. Verified relies on *B.U.S.A. Corp. v. Ecogloves, Inc.*, 2006 WL 3302841 at *4 (S.D.N.Y. Jan. 31, 2006), but in that case the company had spent many years developing the specific contacts at substantial cost, and the list could not easily be duplicated. This is not true here.

Here Fischer brought nearly all the names with him when he first came to work at Verified, and the only names not brought to Verified by Fischer are easily found. (Fischer Decl. ¶¶ 6, 31-35.) Any competent sales manager could compile a list of the senior travel managers of the Fortune 500 companies in a short period even if those persons were previously unknown to him or her. (*Id.* ¶ 9.) What is important is the Registered Traveler product sold, not the universe of easily identifiable major corporate buyers of the product. (*Id.* ¶ 10.) Everyone knows the major airlines, hotel chains, rental car companies, credit-card providers and major corporations most interested in Registered Traveler cards and services. (*Id.* ¶ 11.) Verified's motion for a preliminary injunction is not trying to protect any trade secret; it is seeking to suppress lawful competition.

Sixth, there has been no improper use of the List or any information belonging to Verified. Verified alleges that it was improper for nonparty Kevin Mitchell to send mass emailings (which went to some 10,000 people) to a group that included some people who were at Verified or connected in some way with people at Verified, but the emailings were not based on the List printed by Fischer. (Fischer Decl. ¶ 48; Mitchell Decl. ¶¶ 12, 14.) *None* of the allegedly improperly used names came from Fischer or the List. (Fischer Decl. ¶ 53, Ex. A.) Fischer did not provide email contacts to Mitchell. (Fischer Decl. ¶¶ 46, 53; Mitchell Decl. ¶ 2.)

Seventh, the mass emailings by Mitchell are innocuous and cannot ground any claim by Verified. The first emailing is a preview of a 4-page article written by Mitchell for a magazine.

FLO's name is mentioned only in one paragraph. (Mitchell Decl. ¶ 13.) The second emailing reports a discount offered by FLO. (Mitchell Decl. ¶ 14.) The third emailing includes a survey. (Mitchell Decl. ¶ 15.) They all went to approximately 10,000 contacts and were not targeted in any way connected with the List (which Fischer never provided to Mitchell) or with Verified. (Mitchell Decl. ¶¶ 12-15.) Therefore there is no likelihood that Verified can succeed in showing any trade secret misappropriation.[4]

C. There is no likelihood that Plaintiff will succeed on its claim that Fischer breached his employment agreement with Plaintiff.

Verified, not Fischer, is the only party in breach of the employment agreement between Verified and Fischer. As explained above, Fischer has not misappropriated anything and has not improperly disclosed or used Verified's confidential information. There is no basis for alleging that he has breached his employment agreement.

D. There is no likelihood that Plaintiff will succeed on its other alleged causes of action.

Verified claims in a footnote that it is likely to prevail on other causes of action alleged in its Complaint (Pl. Mem. 21 n.6), but no argument supports this claim. For the reasons explained above, there is no likelihood that Verified will prevail on any of its other alleged causes of action.

The cases cited by Verified do not suggest otherwise. Verified cites *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 832 N.Y.S.2d 873 (2007) (Pl. Mem. 21 n.6), to support its claim for conversion, but *Thyroff* simply states that electronic data can be converted if the plaintiff has been deprived of its use. "[A] defendant who, though having custody of goods, does not 'exclude

---

[4] Verified's brief presents substantive argument on a trade secret claim based only on information allegedly taken by Fischer on December 5, 2006. While the complaint alleges improper statements by Fischer at the Little Rock Airport Commission hearing, these cannot provide any

(footnote continued to next page)

the owner from the exercise of his rights' is not liable for conversion." *State v. Seventh Regiment Fund, Inc.*, 98 N.Y.2d 249, 259-260, 746 N.Y.S.2d 637, 645 (N.Y. 2002) (quoting *Bradley v. Roe*, 282 N.Y. 525, 531-532 (1940)). Verified has never been denied the use of its information.

Verified cites *World Wrestling Fed'n Entm't v. Bozell*, 142 F. Supp. 2d 514, 532 (S.D.N.Y. 2001), to support its claim for tortious interference with Fischer's employment contract, but this case shows that breach of the contract is a necessary element of any interference claim. Verified's claims fails because Fischer has not breached his employment agreement.

Verified says that *Securitron Magnalock Corp. v. Schnabolk*, 65 F.3d 256 (2d Cir. 1995), supports its claim for violations of New York's General Business Law, Section 349(h) for deceptive practices, but this is wrong. *Securitron* holds that to prevail on a § 349 claim, "the gravamen of the complaint must be consumer injury or harm to the public interest." *Securitron*, 65 F.3d at 264 (quoting *Azby Brokerage, Inc. v. Allstate Ins. Co.*, 681 F. Supp. 1084, 1089 n.6 (S.D.N.Y. 1988)). Verified has made only unsupported, conclusory allegations of harm to the public at large and therefore has no claim for violation of § 349. As courts have explained, "[i]njury or harm that satisfy this standard include potential danger to the public health or safety," and "[d]isputes between competitors where the core of the claim is harm to another business as opposed to consumers" do not come within the scope of a § 349 claim. *Gucci America, Inc. v. Duty Free Apparel, Ltd.*, 277 F. Supp. 2d 269, 273 (S.D.N.Y. 2003) (internal quotation marks and citation omitted).

(footnote continued from previous page)
legitimate basis for complaint. As explained above in the fact section of this brief, the full details in Verified's own motion papers refute its claims. (*See supra* pp. 8 - 9.)

E. There are no serious questions going to the merits or balance of hardships favoring a TRO.

Verified is using this litigation to interfere with normal competition. It was timed to coincide with the presentation on competitive bids to the Washington D.C. airport. (Fischer Decl. ¶ 23.) Verified knew or should have known that its claims were baseless, and nothing could justify a preliminary injunction under the "serious questions" and "balance of hardships" test.

F. There is no threat of irreparable harm.

"To establish irreparable harm, plaintiffs must demonstrate an injury that is neither remote nor speculative, but actual and imminent." *Tucker Anthony Realty Corp. v. Schlesinger*, 888 F.2d 969, 975 (2d Cir. 1989) (internal quotations omitted). A preliminary injunction is not appropriate when monetary damages will serve as adequate compensation. *Id.* "The law in this circuit requires a showing that irreparable damages are likely, not merely possible." *Goldblatt v. Englander Communs., LLC*, 431 F. Supp. 2d 420, 425 (S.D.N.Y. 2006); *Iron Mountain Information Management, Inc. v. Taddeo*, 455 F. Supp. 2d 124, 132 (E.D.N.Y. 2006). There can be no threat of irreparable harm when Verified has no colorable misappropriation-of-trade-secrets or other claim.

G. The proposed TRO is vastly overbroad and impermissibly vague.

The exceedingly overbroad and impermissibly vague TRO requested by Verified—among other things preventing the Defendants from "soliciting for business any and all individuals and corporations affiliated with individuals whose contact information was contained on plaintiff's Salesforce Database for a period of six months" (*see* Order to Show Cause")—cannot be grounded in the innocuous List in question and exposes Verified's anti-competitive motives.

IV. There Is No Basis For Expedited Discovery.

There can be no basis for expedited discovery, or even for jurisdiction. If for some reason the Court decides to order expedited discovery, Defendants will need discovery from Verified on many issues. These include, but are not limited to, the following:

(1) The history of the Database.

(2) The source of each name on the List and the basis for Verified's claim that it expended any effort to find those names.

(3) The use, as shown by Verified's computer, email, and other records and the testimony of its employees, that was made of this List.

(4) Verified's stock-option records, including its failure to pay what it owes Fischer.

(5) Verified's use of the contacts information provided by Fischer in January 2007, which was sought by making veiled threats to Fischer.

CONCLUSION

For all the reasons explained above and in the other submissions to the Court, Defendants respectfully request that the Court deny Plaintiff's request for a TRO and expedited discovery.

Dated: July 31, 2007

DLA PIPER US LLP

By: _____

Stanley McDermott (SM 0530)
Michael R. Hepworth (MH 2398)
1251 Avenue of the Americas
New York, New York 10020-1104
(212) 335-4500
Attorneys for defendants Fred Fischer, Saflink Corporation, and FLO Corporation

Exhibit A

Westlaw.

18 U.S.C.A. § 1030

Effective: [See Notes]

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 47--FRAUD AND FALSE STATEMENTS

→§ 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

© 2007 Thomson/West. No Claim to Orig. U.S. Govt. Works.

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; [FN1]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under

© 2007 Thomson/West. No Claim to Orig. U.S. Govt. Works.

subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) [FN2] (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and

(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

© 2007 Thomson/West. No Claim to Orig. U.S. Govt. Works.

18 U.S.C.A. § 1030

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means--

(A) an institution, [FN3] with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

© 2007 Thomson/West. No Claim to Orig. U.S. Govt. Works.

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

[FN1] So in original. Probably should be followed by "or".

[FN2] So in original. Probably should be followed by a comma.

[FN3] So in original. The comma probably should not appear.

Current through P.L. 110-49 approved 07-26-07

Copr. © 2007 Thomson/West. No Claim to Orig. U.S. Govt. Works.

END OF DOCUMENT

© 2007 Thomson/West. No Claim to Orig. U.S. Govt. Works.